Babr24.com

Автор: Владимир Губайловский © Радио Свобода ИНТЕРНЕТ, МИР 👁 2579 21.01.2009, 16:58 👍 276

Умный вирус создает гигантскую зомби-сеть

В Сети происходит самая мощная вирусная эпидемия за последние 5 лет. Вирус уже инфицировал 10 миллионов компьютеров во всем мире, причем в последнюю неделю каждый день он заражал более миллиона машин.

Возможно, идет подготовка в созданию гиганской зомби-сети (ботнета), которая будет использоваться для рассылки спама и атак на сайты.

Вредоносная программа известная под названиями Conficker, Downadup или Kido, согласно антивирусным классификациям разных компаний была впервые идентифицирована в октябре 2008 года. На сегодня она заразила около 10 миллионов компьютеров. Эксперты предупреждают, что в дальнейшем число зараженных машин будет расти, и настоятельно советуют пользователям установить на компьютеры последние «заплатки» к операционной системе Windows.

Вирус проникает в компьютер, используя бреши в операционной системе. Возможно, непосредственным толчком к стремительному росту эпидемии стали Рождественские каникулы, во время которых во многих компаниях отдыхали специалисты по компьютерной безопасности и во время не установили обновления: в результате были поражены крупные корпоративные сети.

Вредоносная программа действует гибко и изобретательно. Она находит на компьютере файл services.exe, используемый операционной системой, и прописывает в него часть своего кода. Себя вирус размещает в виде файла dll под случайным именем. После этого вирус модифицирует системный регистр Registry таким образом, что вредоносный dll в дальнейшем должен загружаться как системный сервис. Кроме того вирус создает на компьютере HTTP-сервер и перезагружает машину. Удалить вредоносный код после этого крайне трудно. Специалисты F-secure говорили, что во многих случаях они видят вредоносный код, но уничтожить его не могут, поскольку он слишком хорошо защищен.

После того как вирус «укоренился» в новом месте он начинает активный обмен с сайтами-хозяевами, загружает новый код и по-видимому готовится к чему-то серьезному. Эксперты F-secure заметили, что вирус ежедневно создает сотни доменных имен, только одно из соответствует сайту с которого идет догрузка вредоносного кода, но отыскать с какого конкретно крайне трудно.

Вирус умеет заражать флеш-память и MP3-плееры. Если зараженный носитель подключить к другому компьютеру – этот компьютер будет заражен; умеет подбирать простые пароли – вроде 12345 или QWERTY.

Компания Microsoft отмечает, что вредоносная программа инфицировала компьютеры во многих частях мира, в том числе большое количество пораженных компьютеров находится в Китае, Бразилии, Индии и России.

Вебпланета, высказала предположение, что Conficker создает гигантскую зомби-сеть (botnet), которая будет управляться из единого центра и использоваться для рассылки спама и DoS-атак. Вебпланета пишет: «Хотя зараженные компьютеры и пытаются регулярно связаться с теми или иными серверами, пока нет свидетельств тому, что они контролируются злоумышленниками и используются в зловредных целях (рассылка спама, кража паролей, DDoS-атаки и т.п.), а следовательно формально не являются ботнетом. Однако весьма вероятно, что рано или поздно эта армия компьютеров начнет действовать».

Специалисты антивирусной компании Trend Micro также считают, что идет подготовка к созданию глобальной зомби-сети.

На сегодня крупнейший ботнет Cutwail подчиняет от 125 до 175 тыс. компьютеров. Если хотя десятая часть компьютеров, уже зараженных Conficker, образует ботнет, это будет самая крупная зомби-сеть в истории интернета.

Эпидемия, охватившая огромный сегмент Сети, опровергает мнение экспертов, которые неоднократно говорили о том, что эпоха массовых эпидемий закончилась, и сегодня злоумышленники сосредоточены на атаках на определенные сайты и хищении номеров кредитных карточек.

По мнению, антивирусных аналитиков пик эпидемии еще не пройден, а последствия ее могут быть тяжелыми.

Автор: Владимир Губайловский © Радио Свобода ИНТЕРНЕТ, МИР 👁 2579 21.01.2009, 16:58 👍 276

URL: https://babr24.com/?ADE=50108 Bytes: 3810 / 3810 Версия для печати Скачать PDF

👍 Порекомендовать текст

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:
- *Телеграм*
- *ВКонтакте*

Связаться с редакцией Бабра:
newsbabr@gmail.com

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com